THE DARK SIDE OF E-COMMERCE: THE EMAIL SPAM EPIDEMIC

by US Senator Charles E. Schumer

Buying products over the Internet or e-commerce has been a boon to both consumers and businesses by driving down costs and prices and continues to grow at a rapid pace. In 2003, almost $50 billion worth of retail shopping took place online according to BizRate.com, an increase of 34% over 2002. Unfortunately, this new virtual market also has a dark side: email spam. In an effort to attract customers, certain online marketers and other Internet sales entrepreneurs send billions of pieces of junk email each year. This annoying and often oppressive sales tactic has reached epidemic proportions, slowing Internet traffic to a crawl, consuming valuable information storage space and needlessly bombarding the in-boxes of users with unwanted email. This report details the scope of the problem in New York State, the types of systems available to combat email spam, while also outlining legislative efforts to curtail the problem.

SPAM IN NEW YORK STATE AND ITS COSTS

According to the Radicati Group, a California-based market research group, 5.7 million people in New York State or 30% of the population have access to email either through their home or workplace.

The Radicati Groups estimates that 2.75 million of these people live in New York City, meaning that the population of email users in New York City is almost as large as the entire population of Chicago, the third-largest city in the United States.

According to Ferris Research, the average email user received 3 pieces of spam email each day in 2002, meaning that email users in New York City received 8.25 million junk emails each day or over 3 billion per year.

WHAT IS EMAIL SPAM?

Email spam refers to any form of *unsolicited* email that users receive from commercial sources. Among the most common forms of spam are advertisements for online gambling services, pornography, herbal remedies or financial schemes, many of which are fraudulent in nature.

Internet users make themselves vulnerable to spam by exposing their email address to online marketers through web sites, news groups, chat rooms, mailing lists and other public sources.

Spammers use software called "spam bots" to harvest email addresses from these public areas. These programs automatically "crawl" the web and locate and record these harvested email addresses into a database to be used for mass junk mailings.

Profile of New York City/State Email Users *Figures given in millions*			
	Total Email Users	**Business**	**Personal**
New York City	2.75	1.51	1.24
New York State	5.7	2.74	2.96

Source: The Radicati Group

Assuming it takes five seconds to identify and delete each piece of spam, New Yorkers spend 4.2 million hours ridding themselves of junk mail each year.

Email users pay dramatic costs for the billions of pieces of spam they receive each year. According to Ferris Research, ISPs spend $5 to $20 per user annually in order to combat spam, a cost they then pass on to Internet users.

New York State has over 4.5 million Internet subscribers, meaning that these users pay ISPs between $22.5 million and $90 million per year in order to prevent spam from reaching their in-boxes.

Individual users can also purchase additional personal spam filters that they install on their personal computers which range in cost from $20 to $40 each.

Ferris Research estimates that spam costs businesses in the United States $10 billion per year from a variety of sources:

i) **lost productivity**: time spent deleting messages and tracking down legitimate messages mistakenly diverted to junk mail folders costs businesses $4 billion per year;

ii) **consumption of IT resources:** staff time and equipment purchases such as more powerful servers, increased bandwidth and disk space required by increasing in spam levels costs businesses $3.7 billion per year;

iii) **help desk incidents**: efforts to eliminate spam or locked in-boxes caused by spam costs businesses $1.3 billion in help-desk activity per year.

FIGHTING BACK

There are a number of ways that Internet Service Providers (ISPs) and users can try and prevent spam from reaching email in-boxes, though none of these is 100% effective:

Filters: ISPs and individuals can use software to block email from specific senders or that contain certain phrases or words. Such filters, however, can be circumvented by spammers who change their sending address after they have been blocked or who deliberately misspell words that nonetheless remain intelligible. For instance, "Viagra" advertising might be successfully blocked by a spam filter, but "Vyagra" would not be blocked by that filter. With the endless

possibilities for such spellings, filters are unable to keep up with the spread of spam. Filters also have the drawback of possibly blocking legitimate email that may nonetheless have phrases or words that the filter was programmed to block.

Blacklists: ISPs that do not actively discourage spam email from being sent from their networks are put on a centrally-maintained blacklist. Other ISPs refuse all Internet traffic from these servers, interrupting spam transmission and punishing ISPs for not discouraging the practice. Unfortunately, because spammers can "relay" spam from a legitimate server, ISPs can become unwittingly involved in spam transmission. Blacklists can therefore penalize innocent ISPs because of reviled spammer behavior.

Source Authentication: This anti-spam mechanism intercepts all email before it reaches your account and requires the original sender to confirm that the intercepted email is not spam by replying to the server's confirmation request. Since spam is usually sent in the thousands from email accounts that are not actively maintained, requests for authentication go unanswered, and the spam never reaches the target account. In addition to adding more traffic to the Internet, these systems often cause a delay in legitimate email delivery and add the cumbersome confirmation-step to the email delivery process.

LEGISLATIVE ACTION

Despite Harris Interactive surveys showing that 80% of Internet users find spam "very annoying" and that 74% favor a legal ban on spam, no federal statute exists regulating its use.

Although 26 states have laws regulating spam – New York is not one of them – these laws have had little success in arresting the spam epidemic because spammers are able operate in states where such laws are not in force.

Senators Conrad Burns and Ron Wyden currently have legislation before that Senate that seeks to eliminate fraud perpetuated over email by requiring marketing email to have a subject heading that accurately reflects the content of the email and which contains a valid address that permits the recipient to "opt-out" of receiving any future correspondence.

While the Burns-Wyden bill is an excellent first step, it still does not go far enough toward resolving the spam problem. A comprehensive approach is required that allows Internet users to automatically opt out of receiving spam, requires spammers to clearly identify their messages as advertising, and contains stiff penalties for violations of these rules.

Senator Schumer is currently drawing up legislation that will put this strategy into effect using a

multi-faceted approach :

The Schumer Anti-Spam Plan

i) **No-Spam List:** As a complement to the Federal Trade Commission (FTC) recently created federal "no-call" registry meant to discourage telemarketers from calling individuals who do not wish to be contacted, the agency should establish a "no-spam" list of email addresses that do not wish to receive spam email. The FTC expects the "no-call" registry to reduce telemarketing calls by 80% while a "no-call" registry in New York State already has 2 million people listed.

ii) **Mandatory Subject Line Identification:** In order to allow recipients and filters to easily identify spam, all junk mail should have the letters "ADV" in the subject line indicating that it contains a message of commercial content.

iii) **Requiring Full Disclosure in Email Headers and Addresses:** Many spammers deliberately use counterfeit addresses, fraudulent domain names, and fake routing information to hide the source of the email. For instance, many spammers send emails that appear to be from America Online accounts but are from entirely different systems. Other spammers use misleading subject lines in their emails to trick readers into opening them. The Schumer legislation will require subject lines and headers to accurately reflect both the source and content of the email message.

iv) **Providing Real "Unsubscribe" Mechanisms and Enforcing Usage:** All commercial emailers will be required to provide an "unsubscribe" feature so recipients can opt out of receiving future messages. While some reputable commercial emailers already do this, many spammers trick recipients by providing what appear to be "unsubscribe" options that in fact put you on lists for new spam. Such practices would be prohibited and penalties imposed for such deception.

v) **Banning Automated Email Address Harvesting:** Spam bots or any other email harvesting will be banned, just as federal legislation that has virtually eliminated unsolicited auto-dial mass faxes that once plagued homes and businesses.

vi) **Stiff Penalties for Non-Compliance:** In order to make spammers comply with the new rules, stiff civil and criminal penalties should be enacted, including potential prison time for repeat offenders.